Lehrstuhl für Algebra und Zahlentheorie
Prof. M. Hien

SS 2012
F. Vogler

Aufgabenblatt 1

Algebra I

Abgabe bis 12:00 Uhr am Freitag, den 20.04.2012

Willkommen zum Studium der Mathematik an der Universität Augsburg!
Jede Woche werden Sie ein Aufgabenblatt bekommen, welches Ihnen Gelegenheit bieten soll den Stoff der Vorlesung zu wiederholen und zu vertiefen. Ziel der Aufgaben ist es zu lernen mathematische Probleme selbständig zu durchdringen, zu lösen und mündlich und schriftlich präzise darzustellen. Bei der Umsetzung dieses Vorhabens werden Sie durch wöchentlich stattfindende Übungen unterstützt, zu welchen Sie sich im Digicampus der Universität Augsburg unter

`https://digicampus.uni-augsburg.de/`

für die Lehrveranstaltung „Einführung in die Algebra“ (SS 2012) anmelden müssen. Anmeldeschluss ist der kommende Freitag um 12:00 Uhr. Sie werden im Laufe diesen Tages über Ihre Zuteilung zu den Übungsgruppen per E-Mail informiert.
Lesen und verinnerlichen Sie den Hinweis auf

`http://www.mathematik.uni-mainz.de/Members/lehn/le/uebungsblatt`

als Leitfaden für den richtigen Umgang mit den Übungsaufgaben!

Aufgabe 1.

(i) Zeigen Sie, dass für zwei Mengen A, B gilt:

$$A \subset B \Longleftrightarrow A \cup B = B \ .$$

(ii) Beweisen Sie das Distributivgesetz für Mengen, d.h. zeigen Sie die Gleichheit

$$S \cup (C \cap D) = (S \cup C) \cap (S \cup D).$$

Bitte wenden!

Aufgabe 2.

(a) Wie viele Äquivalenzrelationen gibt es auf der Menge $\{1, 2, 3\}$?

(b) Es bezeichne $\mathbb{Z}^{\mathbb{Z}}$ die Menge aller Abbildungen von $\mathbb{Z}$ in sich selbst. Wir definieren für $f, g \in \mathbb{Z}^{\mathbb{Z}}$:

$$f \sim g :\Longleftrightarrow f(0) = g(0) \ .$$

Zeigen Sie, dass dies eine Äquivalenzrelation ist und dass das Bild von

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}^{\mathbb{Z}} \ , \ x \mapsto \big(c_x : \mathbb{Z} \to \mathbb{Z} \ , \ z \mapsto c_x(z) := x\big)$$

ein vollständiges, minimales Repräsentantensystem ist.

Aufgabe 3.
Beweisen Sie die folgenden Behauptungen mit

(I) Widerspruch: $\sqrt{p} \notin \mathbb{Q}$ für alle Primzahlen p.

(II) Kontraposition: Ist $2^n - 1$ eine Primzahl ($n \in \mathbb{N}$), so ist n selbst eine Primzahl.

Aufgabe 4.
Für eine Menge M bezeichne $\mathfrak{P}(M)$ die *Potenzmenge*, das ist per Definition die Menge

$$\mathfrak{P}(M) := \{A \subset M \mid A \text{ ist Teilmenge von } M\}$$

aller Teilmengen von M. Zeigen Sie:

(α) Ist $f : M \to N$ eine Abbildung, so ist durch die Definition des *Urbilds* eine Abbildung

$$\Phi : \mathfrak{P}(N) \longrightarrow \mathfrak{P}(M) \ , \ B \mapsto f^{-1}(B)$$

definiert.

(β) In obiger Situation gilt:

$$f \text{ ist surjektiv } \Longleftrightarrow \Phi \text{ ist injektiv.}$$

Lehrstuhl für Algebra und Zahlentheorie
Prof. M. Hien

SS 2012
F. Vogler

Aufgabenblatt 2

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 27.04.2012

Aufgabe 1. 4 PUNKTE

(a) Wie viele Äquivalenzrelationen gibt es auf der Menge $\{1,2,3\}$?

(b) Es bezeichne $\mathbb{Z}^{\mathbb{Z}}$ die Menge aller Abbildungen von $\mathbb{Z}$ in sich selbst. Wir definieren für $f, g \in \mathbb{Z}^{\mathbb{Z}}$:

$$f \sim g :\Longleftrightarrow f(0) = g(0) \ .$$

Zeigen Sie, dass dies eine Äquivalenzrelation ist und dass das Bild von

$$\psi : \mathbb{Z} \longrightarrow \mathbb{Z}^{\mathbb{Z}} \ , \ x \mapsto (c_x : \mathbb{Z} \to \mathbb{Z}, \, z \mapsto c_x(z) := x)$$

ein vollständiges, minimales Repräsentantensystem ist.

Aufgabe 2. (4 PUNKTE)
Es sei $\equiv \bmod m$ die in der Vorlesung eingeführte Kongruenzrelation modulo m und $\mathbb{Z}/m\mathbb{Z}$ die Menge der zugehörigen Äquivalenzklassen (die Restklassen modulo m). Wir setzen:

$$[r] \cdot [s] := [rs]$$

für Elemente $[r], [s] \in \mathbb{Z}/m\mathbb{Z}$. Beweisen Sie, dass die so auf $\mathbb{Z}/m\mathbb{Z}$ eingeführte Multiplikation *wohldefniert* ist, d.h. dass aus $r \equiv r' \bmod m$ und $s \equiv s' \bmod m$ folgt, dass $rs \equiv r's' \bmod m$.

Aufgabe 3. (4 PUNKTE)
Seien $A, B \neq \emptyset$ und $f : A \to B$ eine Abbildung. Mit $\mathrm{id}_A : A \to A$ bezeichnen wir die Identitätsabbildung mit $\mathrm{id}_A(x) = x$ für alle $x \in A$.

(a) Zeigen Sie: Genau dann existiert eine Abbildung $g \colon B \to A$ mit $g \circ f = \mathrm{id}_A$, wenn f injektiv ist. In diesem Falle heißt g *Linksinverse zu* f (oder auch *Retrakt*).

(b) In der Vorlesung wurde für eine zusätzliche Abbildung $g : B \to C$ bewiesen:

$$g \circ f \text{ bijektiv } \Longrightarrow f \text{ injektiv und } g \text{ surjektiv.}$$

Geben Sie ein Beispiel an, dass zeigt, dass die Umkehrung davon falsch ist.

Aufgabe 4. (4 Punkte)
Es sei G eine Gruppe. Beweisen Sie, dass die folgenden Aussagen äquivalent sind:

(α) G ist abelsch.

(β) Es gilt $(ab)^2 = a^2b^2$ für alle $a, b \in G$.

(γ) Es gilt $(ab)^{-1} = a^{-1}b^{-1}$ für alle $a, b \in G$.

Lehrstuhl für Algebra und Zahlentheorie | SS 2012
Prof. M. Hien | F. Vogler

Aufgabenblatt 3

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 04.05.2012

Aufgabe 1. (4 Punkte)
Es sei G eine Gruppe mit dem neutralen Element e.

(i) Sei $g \in G$ ein Element der Ordnung 2 (d.h. es ist $g \neq e$, aber $g^2 = e$). Begründen Sie, weshalb $g = g^{-1}$ gilt.

(ii) Beweisen Sie: Ist G endlich und $|G|$ gerade, so enthält G mindestens ein Element g der Ordnung 2.

In der Vorlesung wurde die symmetrische Gruppe $S(n)$ auf n Ziffern eingeführt. Eine Permutation $\tau \in S(n)$ heißt für $k \geq 2$ ein *Zyklus der Länge k* oder *k-Zyklus*, falls es paarweise verschiedene Zahlen $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$ gibt, so dass $\tau(a_i) = a_{i+1}$ für $1 \leq i < k$, $\tau(a_k) = a_1$ und $\tau(a) = a$ für alle $a \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$. In dieser Situation verwendet man die Schreibweise $\tau = (a_1, \ldots, a_k)$ für den k-Zyklus.
Zwei Zyklen $(a_1, \ldots, a_k)$ und $(b_1, \ldots, b_l)$ heißen *disjunkt* oder *fremd*, wenn

$$\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$$

gilt.

Aufgabe 2. (4 Punkte)
Aus der symmetrischen Gruppe $S(7)$ seien folgende Permutationen gegeben:

$$\pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 3 & 5 & 1 & 4 \end{pmatrix} \text{ und } \sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 6 & 3 & 7 & 1 \end{pmatrix}.$$

Berechnen Sie $\rho := \pi\sigma^{-1}$ und stellen Sie ρ als Komposition fremder Zyklen dar!

Aufgabe 3. (4 Punkte)
Beweisen Sie:

(a) Ist $\xi \in S(n)$ ein Zyklus der Länge k und $\pi \in S(n)$ beliebig, so ist auch $\pi^{-1}\xi\pi$ ein Zyklus der Länge k.

(b) Zu zwei Zyklen ξ_1, ξ_2 gleicher Länge aus $S(n)$ gibt es eine Permutation $\pi \in S(n)$ mit $\xi_2 = \pi^{-1}\xi_1\pi$.

Für die folgende Aufgabe benötigen Sie den Begriff der Matrix. Dieser wird kommenden Mittwoch in der Vorlesung eingeführt. Sie können aber die Aufgabe auch schon früher bearbeiten: Recherchieren Sie, wie die Addition und Multiplikation von Matrizen funktioniert und wagen Sie sich ans Werk!

Aufgabe 4. (4 Punkte)
Wir definieren mit

$$\mathcal{C} := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \,\middle|\, x, y \in \mathbb{R} \right\}$$

eine Teilmenge der (2×2)-Matrizen $\mathbb{R}^{2\times 2}$ über den reellen Zahlen.

(a) Weisen Sie nach, dass $\mathcal{C}$ eine abelsche Gruppe bezüglich der Addition ist und bestimmen Sie das neutrale Element!

(b) Untersuchen Sie, ob $\mathcal{C}$ auch eine Gruppe bezüglich der Matrixmultiplikation ist! Falls dem so ist, handelt es sich dann um eine abelsche Gruppe?

(c) Wir definieren die Menge $\mathbb{C} := \{a + \mathrm{i}b \mid a, b \in \mathbb{R},\ \mathrm{i}^2 = -1\}$ und die Abbildung

$$F \colon \mathbb{C} \to \mathcal{C}\,, \quad a + \mathrm{i}b \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Rechnen Sie nach, dass F eine $\mathbb{R}$-lineare[1] Abbildung ist!
Ist F auch *multiplikationstreu*[2]?

[1] $\mathbb{R}$-linear heißt: $(\forall r \in \mathbb{R})(\forall a, b \in \mathbb{C})\colon F(ra) = rF(a)$ und $F(a + b) = F(a) + F(b)$.
[2] Multiplikationstreue heißt hier: $\forall z, z' \in \mathbb{C}\colon F(zz') = F(z)F(z')$.

Lehrstuhl für Algebra und Zahlentheorie
Prof. M. Hien

SS 2012
F. Vogler

Aufgabenblatt 4

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 11.05.2012

Aufgabe 1. (4 Punkte)
Es sei G eine Gruppe mit dem neutralen Element e. Beweisen Sie: Enthält G nur ein einziges Element g der Ordnung 2, so gilt $gx = xg$ für alle $x \in G$.

Aufgabe 2. (4 Punkte)
Welche der folgenden Abbildungen sind linear?

$$A_1 \colon \mathbb{R}^3 \to \mathbb{R}^2 \ \text{ mit } \ A_1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} x \\ 2z \end{pmatrix}.$$

$$A_2 \colon \mathbb{R}^3 \to \mathbb{R}^3 \ \text{ mit } \ A_1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} x+1 \\ y+2 \\ z+3 \end{pmatrix}.$$

$$A_3 \colon \mathbb{R}^3 \to \mathbb{R}^3 \ \text{ mit } \ A_1 \begin{pmatrix} x \\ y \\ z \end{pmatrix} := \begin{pmatrix} x+y \\ -x \\ 2z \end{pmatrix}.$$

$$A_4 := A_1 \circ A_3.$$

Geben Sie im Falle der Linearität die zugehörige Matrix an!

Aufgabe 3. (4 Punkte)
Sei die Matrix

$$B := \begin{pmatrix} 2 & -1 & 0 & 1 \\ -1 & 6 & -1 & 4 \\ 5 & 3 & 2 & 0 \end{pmatrix}$$

gegeben. Berechnen Sie $B \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$!

Aufgabe 4. (4 Punkte)
Es sei G eine Gruppe. Beweisen Sie die folgenden Behauptungen!

(i) Sind H und H' Untergruppen von G, so ist $H \cap H'$ eine Untergruppe von G.

(ii) Sei I eine Menge und $(H_i)_{i\in I}$ eine Familie von Untergruppen. Dann ist

$$\bigcap_{i\in I} H_i \subset G$$

eine Untergruppe.

(iii) Sei $g \in G$ ein Element und $\Psi_g := \{H \subset G \mid H \text{ ist Untergruppe und } g \in H\}$. Setze

$$<g> := \bigcap_{H\in\Psi_g} H.$$

Dann gilt:

$$<g> = \left\{g^k \mid k \in \mathbb{Z}\right\}.$$

(Dabei ist $g^k = \underbrace{g\cdots g}_{k\text{-mal}}$ für $k > 0$ und $g^k = \underbrace{g^{-1}\cdots g^{-1}}_{|k|\text{-mal}}$ für $k < 0$.)

Lehrstuhl für Algebra und Zahlentheorie | SS 2012
Prof. M. Hien | F. Vogler

Aufgabenblatt 5

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 18.05.2012

Aufgabe 1. (4 Punkte)
Wir betrachten die symmetrische Gruppe $S(3)$ auf drei Ziffern. Sei $\sigma \in S(3)$ der 2-Zyklus $(1, 2)$. Zeigen Sie: Jeder Versuch den Gruppenquotienten $S(3)/<\sigma>$ mit einer Gruppenstruktur zu versehen, so dass die kanonische Projektion

$$\pi \colon S(3) \to S(3)/<\sigma>$$

ein Gruppenhomomorphismus wird, scheitert.

Aufgabe 2. (4 Punkte)
Es sei G eine Gruppe. Für $g \in G$ sei die Ordnung $\mathrm{ord}(g)$ von g definiert als die Mächtigkeit der von g erzeugten Untergruppe in G, d.h. $\mathrm{ord}(g) := |<g>|$.
Beweisen Sie: Ist $\mathrm{ord}(g) < \infty$, so gelten die folgenden Aussagen.

(a) $\mathrm{ord}(g) = \min \{n \in \mathbb{N} \mid g^n = e\}$.

(b) $g^n = e \Leftrightarrow \mathrm{ord}(g) \mid n$.

(c) $<g> = \left\{e = g^0, g^1, g^2, \ldots, g^{\mathrm{ord}(g)-1}\right\}$.

(d) $\mathrm{ord}(g^k) = \frac{\mathrm{ord}(g)}{\mathrm{ggT}(k, \mathrm{ord}(g))}$ für $k \in \mathbb{N}$.

Aufgabe 3. (4 Punkte)
Es Sei G eine Gruppe. Beweisen Sie:

(a) Sind N_1 und N_2 Normalteiler von G mit $N_1 \cap N_2 = \{e\}$, so gilt $n_1 n_2 = n_2 n_1$ für alle $n_1 \in N_1$, $n_2 \in N_2$.

(b) Sei U eine Untergruppe von G der Ordnung $n \in \mathbb{N}$. Ist U die einzige Untergruppe der Ordnung n, so ist U ein Normalteiler von G.

Aufgabe 4. (4 Punkte)
Es sei G eine Gruppe. Beweisen Sie:

(a) Hat $U < G$ den Index 2, so ist U ein Normalteiler in G.

(b) Das Zentrum $\mathrm{Z}(G) := \{g \in G \mid \forall_{h \in G}\ gh = hg\}$ von G ist ein Normalteiler in G.

(c) Die Kerne der Gruppenhomomorphismen sind genau die Normalteiler.

Aufgabe 5. (4 Punkte)
Es sei G eine Gruppe, U eine Untergruppe und $N \subset U$ ein Normalteiler von G. Beweisen Sie:

(a) N ist auch ein Normalteiler von U, und U/N ist eine Untergruppe von G/N.

(b) Ist auch U eine Normalteiler von G, so ist U/N eine Normalteiler von G/N und es gilt:
$$(G/N)/(U/N) \cong G/U.$$

Lehrstuhl für Algebra und Zahlentheorie SS 2012
Prof. M. Hien F. Vogler

Aufgabenblatt 6

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 25.05.2012

Aufgabe 1. (4 Punkte)
Sei $m \in \mathbb{N}$ eine natürliche Zahl. Wir betrachten die auf Aufgabenblatt 2 eingeführte Multiplikation auf der Menge $\mathbb{Z}/(m) := \mathbb{Z}/m\mathbb{Z}$ der Restklassen modulo m.

(a) Zeigen Sie: Ist $a \in \mathbb{Z}$ zu m teilerfremd, so ist jedes Element aus der Restklasse $[a] \in \mathbb{Z}/(m)$ zu m teilerfremd.
Wir nennen dann $[a]$ eine zu m *teilerfremde* (oder auch *prime*) Restklasse.

(b) Weisen Sie nach: Die zu m teilerfremden Restklassen bilden bezüglich der Restklassenmultiplikation eine abelsche Gruppe.

(c) Beweisen Sie: Genau dann gibt es in $\mathbb{Z}/(m)$ mit $m > 1$ zu jeder Restklasse $[r] \neq [0]$ eine Restklasse $[s]$ mit $[r][s] = [1]$, wenn m eine Primzahl ist.

(d) Stellen Sie eine Multiplikationstafel der Gruppe der zu 12 primen Restklassen auf!

(e) Begründen Sie, weshalb es sich bei $(\mathbb{Z}/(m), +, \cdot)$ um einen kommutativen Ring mit Eins handelt! Was heißt hier „kommutativ“?

(f) Ist $\mathbb{Z}/(m)$ ein Integritätsbereich?

Aufgabe 2. (4 Punkte)
Sei R die Potenzmenge einer nichtleeren Menge M. Wir definieren zwei Abbildungen

$$+, \cdot \colon R \times R \to R$$

vermöge

$$A + B := (A \cup B) \setminus (A \cap B)$$

und

$$A \cdot B := A \cap B.$$

Verifizieren Sie, dass R bzgl. der so definierten Verknüpfungen ein kommutativer Ring mit Einselement wird und $A + A = \emptyset$ und $A^2 = A$ für alle Elemente $A \in R$ gilt.

Aufgabe 3. (4 Punkte)
Finden Sie den größten gemeinsamen Teiler der Polynome f und g über $\mathbb{Q}[X]$ und bestimmen Sie eine Darstellung des größten gemeinsamen Teilers durch f und g mit Bézoutkoeffizienten[1].

(a) $f(X) = X^4 + 3X^3 + 4X^2 - 2X - 6\,,\ g(X) = X^2 - 1$.

(b) $f(X) = X^3 - 3X - 1\,,\ g(X) = X^2 + X + 1$.

Aufgabe 4. (4 Punkte)
Ein kommutativer Ring R heißt *euklidischer Ring*[2], falls eine Abbildung

$$\varphi\colon R \setminus \{0\} \to \mathbb{N}_0$$

derart existiert, dass gilt:

(e1) für $a, b \in R$ mit $ab \neq 0$ gilt $\varphi(a) \leq \varphi(ab)$;

(e2) für $a, b \in R$ und $b \neq 0$ existieren $q, r \in R$ so, dass $a = qb + r$ mit $r = 0$ oder $r \neq 0$ und $\varphi(r) < \varphi(b)$.

Wir definieren eine Abbildung auf dem Poylynomring über den ganzen Zahlen, *die Auswertung in* i:

$$\mathrm{ev}_{\mathrm{i}}\colon \mathbb{Z}[X] \to \mathbb{Z}[\mathrm{i}]$$

durch

$$f(X) \mapsto f(\mathrm{i})$$

und nennen $\mathbb{Z}[\mathrm{i}]$ den *Ring der Gaußschen Zahlen.*
Beweisen Sie, dass die Gleichheit $\mathbb{Z}[\mathrm{i}] = \left\{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\,,\ \mathrm{i}^2 = -1\right\}$ gilt und weisen Sie nach, dass $\mathbb{Z}[\mathrm{i}]$ vermöge $\varphi\colon \mathbb{Z}[\mathrm{i}] \setminus \{0\} \to \mathbb{N}_0\,,\ a + \mathrm{i}b \mapsto a^2 + b^2$ ein euklidischer Ring ist!
(Hinweis: Deuten Sie den Quotienten $\frac{u}{x}$ zweier Zahlen $u, v \in \mathbb{Z}[\mathrm{i}]$ geometrisch in der komplexen Zahlenebene und finden Sie eine geeignete Approximation in $\mathbb{Z}[\mathrm{i}]$.)

[1] Damit ist eine Darstellung $\mathrm{ggT}(f, g) = af + bg$ mit geeigneten a und b gemeint.
[2] Der Ring $\mathbb{Z}$ der ganzen Zahlen mit $\varphi(x) := |x|$ ist ein euklidischer Ring.

Lehrstuhl für Algebra und Zahlentheorie SS 2012
Prof. M. Hien F. Vogler

Aufgabenblatt 7

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 01.06.2012

Aufgabe 1. (4 PUNKTE)
Ein Ring[1] R heißt *lokal*, falls er genau ein maximales Ideal besitzt.
Zeigen Sie, dass R genau dann lokal ist, wenn $\mathfrak{m} = R \setminus R^\times$ ein Ideal ist!

Aufgabe 2. (4 PUNKTE)
Sei R ein Integritätsbereich. Anstelle des Polynomringes $R[X]$ über R können wir auch auf der Menge

$$R[[X]] := \{(a_0, a_1, \dots) \mid a_k \in R \text{ für alle } k \geq 0\}$$

der nicht notwendig abbrechenden Folgen eine Ringstruktur durch dieselben Verknüpfungen definieren. Statt $(a_j)_j \in R[[X]]$ schreiben wir formal $\sum_{j=0}^\infty a_j X^j$. Dann gilt die aus der Analysis geläufige Regel

$$\left(\sum_{i=0}^\infty a_i X^i\right) \cdot \left(\sum_{j=0}^\infty b_j X^j\right) = \sum_{k=0}^\infty \left(\sum_{i+j=k} a_i b_j\right) X^k,$$

die Cauchy-Multiplikation.
Es heißt $R[[X]]$ *der Ring der formalen Potenzreihen über R.*
Beweisen Sie die folgenden Behauptungen!

(α) Ist $f = 1 - X$ und $g = \sum_j X^j$, so gilt $fg = 1$.

(β) Ist $f = \sum_j a_j X^j \in R[[X]]$ mit $a_0 \in R^\times$, so existiert $g \in R[[X]]$ mit $fg = 1$.

(γ) Ist K ein Körper und $f = \sum_j a_j X^j \in K[[X]]$ mit $a_0 \neq 0$, so existiert $g \in K[[X]]$ mit $fg = 1$.

---

[1] Ringe in den Übungsaufgaben können, falls nicht anders betont, immer als kommutativ mit Eins angenommen werden.

Aufgabe 3. (4 Punkte)

(a) Sei R ein Ring. Zeigen Sie, dass Nullteiler in R keine Einheiten sind!

(b) Weisen Sie nach, dass ein Ringhomomorphismus $\varphi\colon R \to A$ zwischen beliebigen Ringen Einheiten auf Einheiten abbildet!
Formulieren Sie eine Aussage für die Umkehrung! Gilt diese?

(c) Sei K ein Körper. Beweisen Sie: Jeder Ringhomomorphismus $\phi\colon K \to R$ ist entweder die Nullabbildung oder injektiv.
Was kann daraus für Körperhomomorphismen geschlossen werden?

Aufgabe 4. (4 Punkte)
Sei A ein Hauptidealring. Zeigen Sie, dass jedes von Null verschiedene Primideal in A schon ein maximales Ideal ist!

Lehrstuhl für Algebra und Zahlentheorie — SS 2012
Prof. M. Hien — F. Vogler

Aufgabenblatt 8

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 08.06.2012

Aufgabe 1. (4 Punkte)
Sei R ein kommutativer Ring mit Eins und $R[X]$ der Polynomring in einer Veränderlichen über R. Ferner sei $\mathfrak{p} \subset R$ ein Primideal in R. Beweisen Sie, dass $\mathfrak{p}R[X]$ ein Primideal in $R[X]$ ist!

Aufgabe 2. (4 Punkte)
Sei $\varphi\colon R \to S$ ein Ringhomomorphismus, I ein Ideal in R und J ein Ideal in S.

(a) Zeigen Sie, dass $\varphi^{-1}(J)$ ein Ideal in R ist, welches $\ker \varphi$ enthält!

(b) Beweisen Sie: Wenn φ ein Ringepimorphismus[1] ist, dann ist $\varphi(I)$ ein Ideal in S. Gilt dies auch, wenn φ nicht surjektiv ist?

(c) Untersuchen Sie die Situation aus Teil (b) für den Fall, dass I ein Primideal in R ist!

Aufgabe 3. (4 Punkte)
Sei R ein kommutativer Ring ohne Eins und ohne Nullteiler. Sei S ein Ring, dessen additive Gruppe $R \times \mathbb{Z}$ ist. Die Multiplikation auf S ist dabei durch

$$(r, z) \cdot (\rho, \zeta) = (r\rho + r\zeta + \rho z, z\zeta)$$

gegeben.
Definiere

$$A := \{(r, n) \in S \mid rx + nx = 0 \text{ für jedes } x \in R\}.$$

Beweisen Sie die folgenden Behauptungen!

(a) A ist ein Ideal in S.

(b) S/A besitzt eine Eins und enthält einen Unterring isomorph zu R.

(c) S/A ist nullteilerfrei.

[1] Ein surjektiver Ringhomomorphismus heißt *Ringepimorphismus*.

Aufgabe 4. (4 Punkte)
Es sei an die klassische Version des *Chinesischen Restsatzes* erinnert:
Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ paarweise teilerfremde Zahlen und $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ beliebig. Dann gibt es ein $x \in \mathbb{Z}$ mit

$$x \equiv x_k \mod a_k$$

(also $x - x_k \in a_k\mathbb{Z}$) für alle $k \in \{1, \ldots, n\}$.
Ist $x \in \mathbb{Z}$ eine solche Lösung, so ist

$$x + a_1 \cdots a_n\mathbb{Z} = \{x + k \cdot a_1 \cdots a_n \mid k \in \mathbb{Z}\}$$

die Menge aller Lösungen.

(a) Leiten Sie die klassische Version des Chinesischen Restsatzes aus der eleganten Form der Vorlesung ab, d.h. zeigen Sie, dass

$$\bigcap_{k=1}^{n} a_i\mathbb{Z} = (a_1 \cdots a_n)\mathbb{Z}$$

gilt!

(b) Ein Bauer möchte alle seine Kühe auf einem Volksfest präsentieren. Wenn er sie aber in 3er-Reihen aufstellt, bleiben 2 Kühe übrig. Stellt er sie in 4er-Reihen auf, bleibt eine Kuh übrig. Erst mit 7er-Reihen bleibt keine Kuh mehr übrig. Wie viele Kühe hat der Bauer mindestens?

Lehrstuhl für Algebra und Zahlentheorie
Prof. M. Hien

SS 2012
F. Vogler

Aufgabenblatt 9

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 15.06.2012

Aufgabe 1. (4 Punkte)
Sei K ein Körper und $n \in \mathbb{N}$ eine natürliche Zahl. Wir definieren

$$\mathscr{W} := \{f \in K[X] \mid \deg f \leq n\}$$

als die Menge aller Polynome über K vom Grade kleiner gleich n.

(a) Zeigen Sie, dass $\mathscr{W}$ ein K-Vektorraum ist!
Ist $\mathscr{W}$ auch ein Ring? Begründen Sie *kurz* Ihre Antwort!

(b) Beweisen Sie, dass $\dim_K \mathscr{W} = n + 1$ gilt!

(c) Zeigen Sie, dass

$$\mathscr{B} := \left(1, X + 1, X^2 + X, \ldots, X^n + X^{n-1}\right)$$

ein linear unabhängiges System[1] von Vektoren in $\mathscr{W}$ bildet!
Warum folgt sofort, dass $\mathscr{B}$ eine Basis von $\mathscr{W}$ bildet?

Aufgabe 2. (4 Punkte)
Sei F eine Körpererweiterung von K. Beweisen Sie die folgenden Behauptungen!

(a) Es gilt genau dann $[F : K] = 1$, wenn $F = K$ gilt.

(b) Wenn $[F : K]$ prim ist, dann gibt es keine echten Zwischenerweiterungen.

(c) Falls $u \in F$ den Grad n besitzt, so ist n ein Teiler von $[F : K]$.

Aufgabe 3. (4 Punkte)
Im Körper $\mathbb{C}$ betrachten wir $\mathbb{Q}(\mathrm{i})$ und $\mathbb{Q}(\sqrt{2})$. Zeigen Sie, dass $\mathbb{Q}(\mathrm{i})$ und $\mathbb{Q}(\sqrt{2})$ als $\mathbb{Q}$-Vektorräume isomorph sind, nicht aber als Körper.

---

[1] Wir bezeichnen eine Menge von Vektoren als System, wenn die Reihenfolge der Elemente eine Rolle spielt.

Aufgabe 4. (4 Punkte)
Sei L eine Körpererweiterung über dem Körper K und $v, y \in L$ algebraisch über K. Ferner sei y vom Grad m über K.
Zeigen Sie, dass

$$[K(v, y) : K(v)] \leq m$$

gilt!

Aufgabe 5. (Fakultative Zusatzaufgabe)
Beweisen Sie die Starrheit von $\mathbb{Q}$, d.h. der einzige Automorphismus[2] von $\mathbb{Q}$ ist die Identität.

[2] Ein Automorphismus eines Körpers ist ein bijektiver Körperhomomorphismus des Körpers auf sich selbst.

Lehrstuhl für Algebra und Zahlentheorie
Prof. M. Hien

SS 2012
F. Vogler

Aufgabenblatt 10

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 22.06.2012

Aufgabe 1. (4 Punkte)
Sei $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$ gegeben. Es ist f irreduzibel über $\mathbb{Q}$, besitzt aber eine reelle Nullstelle $u \in \mathbb{R}$.

(a) Welchen Grad besitzt u über den rationalen Zahlen?

(b) Geben Sie eine (möglichst einfache) $\mathbb{Q}$-Basis von $\mathbb{Q}(u)$ an!

(c) Stellen Sie das Element $w := u^4 + 2u^3 + 3 \in \mathbb{Q}[u]$ als Linearkombination in der Basis aus (b) dar.

(d) Berechnen Sie w^{-1} in $\mathbb{Q}[u]$, d.h. drücken Sie w^{-1} in der $\mathbb{Q}$-Basis aus Aufgabenteil (b) aus.

Aufgabe 2. (4 Punkte)
Sei $F|K$ eine beliebige Körpererweiterung und $u, x \in F$ zwei Elemente. Im Körper $K(x)$ gelte

$$u = \frac{x^3}{x+1}.$$

Zeigen Sie, dass $K(x)$ eine einfache Körpererweiterung von $K(u)$ ist!
Was ist $[K(x) : K(u)]$?

Aufgabe 3. (4 Punkte)
Seien $v, y \in L$ algebraisch über K, v vom Grade n und y vom Grade m.
Beweisen Sie die nachstehenden Behauptungen!

(a) Es gilt $[K(v, y) : K] \leq n \cdot m$.

(b) Falls $\mathrm{ggT}(n, m) = 1$, so ist $[K(v, y) : K] = n \cdot m$.

Aufgabe 4. (8 Punkte)
Se $n \in \mathbb{N}$ eine natürliche Zahl. Ein Körper K heißt *von Charakteristik* n, falls n die kleinste natürliche Zahl ist, so dass

$$n \cdot 1 = 1 + \cdots + 1 = 0$$

gilt. (Man sagt auch: die additive Gruppe von K hat die Ordnung n.) Ein Körper ist *von Charakteristik* 0, falls $n \cdot 1 \neq 0$ für alle natürlichen Zahlen n.

(a) Was hat die Charakteristik eines Körpers mit Nullteilern zu tun?

(b) Zeigen Sie, dass K genau dann von Charakteristik n ist, wenn der Kern des einzigen (warum?) Ringhomomorphismus' $\mathbb{Z} \to K$ durch das Hauptideal (n) gegeben ist.
Was gilt folglich, wenn der Kern das Nullideal ist?

(c) Beweisen Sie: Die Charakteristik eines Körpers ist immer eine Primzahl oder Null.

(d) Der Primkörper P von K ist definiert (vgl. Definition 8.2 in der Vorlesung) als der Durchschnitt aller Teilkörper von P. Weisen Sie folgende Behauptung nach:

$$P \cong \mathbb{F}_p \Leftrightarrow \mathrm{Char}(K) = p,$$

wobei $\mathbb{F}_p := \mathbb{Z}/(p)$ bekanntlich (Begründung?) ein Körper ist.

(e) Folgern Sie aus dem bisher Bewiesenen den Satz 8.3 (2) der Vorlesung: Ein Primkörper eines Körpers K ist isomorph zu $\mathbb{F}_p$ oder $\mathbb{Q}$!

(f) Schließen Sie nun: Ein endlicher Körper[1] von Charakteristik p hat p^n Elemente (dabei ist n eine natürliche Zahl).

[1] Ein Körper heißt *endlich*, falls er nur aus endlich vielen Elementen besteht.

Aufgabenblatt 11

Algebra I

Abgabe bis 14:00 Uhr am Freitag, den 29.06.2012

Aufgabe 1. (4 Punkte)
Sei R ein faktorieller Ring und K sein Quotientenkörper. Beweisen Sie die folgenden Aussagen!

(a) Sei $f \in R[X]$. Ist f primitiv und prim in $K[X]$, so ist f prim in $R[X]$.

(b) Der Polynomring $R[X]$ über R ist faktoriell.

Aufgabe 2. (4 Punkte)
Wir wollen in dieser Aufgabe die Diskussion aus der Vorlesung zu Bemerkung (2) beim Eisensteinkriterium aufgreifen.

(a) Beweisen Sie, dass ein Isomorphismus $\varphi\colon R \to S$ zwischen nullteilerfreien Ringen Primelemente bewahrt und Primalität reflektiert!

(b) Sei A ein Integritätsbereich und $R = S = A[X]$. Zeigen Sie, dass $\varphi\colon R \to S$, gegeben durch $f(X) \mapsto f(X + a)$ für $a \in A$, ein Isomorphismus ist. Folgern Sie, dass $f(X) \in A[X]$ genau dann irreduzibel ist, wenn $f(X + a) \in A[X]$ irreduzibel ist.
Welche Konsequenzen hat dies für das Eisensteinkriterium?

Aufgabe 3. (4 Punkte)

(a) Finden Sie alle irreduziblen Polynome vom Grad kleiner gleich vier in $\mathbb{F}_2[X]$!

(b) Untersuchen Sie
$$f := X^5 - X^3 - 1$$
auf Irreduzibilität in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$!

Aufgabe 4. (4 Punkte)
Sei $\overline{\mathbb{Q}}$ ein algebraischer Abschluss der rationalen Zahlen. Finden Sie alle $\mathbb{Q}$-Homomorphismen

$$\mathbb{Q}\left(\sqrt[4]{2}, \mathrm{i}\right) \to \overline{\mathbb{Q}}$$

d.h. bestimmen Sie alle Elemente in $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})|\mathbb{Q})$!

Aufgabe 5. (Faklutativ: Irreduzibilität)
Sei K ein Körper. Wir betrachten den Polynomring $K(X)[Y]$ in einer Veränderlichen Y über dem Funktionenkörper $K(X)$.
Seien $f(Y)$ und $g(Y)$ aus $K[Y]$ teilerfremd mit $\deg(f \cdot g) \geq 1$. Beweisen Sie, dass

$$f(Y) - g(Y)X \in K(X)[Y]$$

irreduzibel ist!